KEYWORD: Security Violations

DIGEST: Applicant, a retired navy Electronic Material Officer with extensive experience handling classified information, self-reported several security violations at his work site between 1999 and 2002. He has accepted responsibility for leaving his office safe unlocked once, and as team leader, for missing documents. He inadvertently transported two "NATO confidential" messages, and once an improperly classified diskette. He recommended an upgrade in his company contract, and a change in its method used to inventory messages to prevent additional security violations. Clearance is granted.

CASENO: 04-07452.h1

DATE: 05/16/2006

DATE: May 16, 2006

In re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 04-07452

DECISION OF ADMINISTRATIVE JUDGE

MARY E. HENRY

APPEARANCES

FOR GOVERNMENT

Richard Stevens, Esq., Department Counsel

FOR APPLICANT

Michael F. Fasanaro, Esq.

SYNOPSIS

Applicant, a retired Navy Electronic Material Officer with extensive experience handling classified information, self-reported several security violations at his work site between 1999 and 2002. He has accepted responsibility for leaving his office safe unlocked once, and as team leader, for missing documents. He inadvertently transported two "NATO confidential" messages, and once an improperly classified diskette. He recommended an upgrade in his company contract, and a change in its method used to inventory messages to prevent additional security violations. Clearance is granted.

STATEMENT OF THE CASE

On September 7, 2005, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry*, dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified, issued a Statement of Reasons (SOR) to Applicant. The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Specifically, the SOR set forth security concerns arising under Guideline K (Security Violations) of the Directive. DOHA recommended the case be referred to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. On October 3, 2005, Applicant submitted a notarized response to the allegations. He requested a hearing.

This matter was assigned to me on January 30, 2006. A notice of hearing was issued on March 6, 2006, and a hearing was held on March 27, 2006. Twelve government exhibits and two Applicant exhibits were admitted into evidence. The record was held open until April 27, 2006 for Applicant to submit additional evidence, which was received on April 10, 2006. The government did not object to the admission of this evidence as Applicant Exhibit C. Applicant and three

witnesses testified. The hearing transcript (Tr.) was received on April 7, 2006.

FINDINGS OF FACT

Applicant denied all the allegations under Guideline K, subparagraphs 1.a. through 1.g. of the SOR.[(1)] After a complete review of the evidence in the record and upon due consideration, I make the following additional findings of fact:

Applicant is a 61-year-old senior analyst for a defense contractor.[(2)] He has worked for this contractor and its predecessor for more than eleven years.[(3)] He completed a security clearance application (SF 86) in November 2002.[(4)]

Applicant enlisted in the United States Navy in 1964, at the age of 19.[(5)] He took numerous training courses offered by the Navy.[(6)] In 1980, the Navy commissioned him an Ensign, and assigned him communications duties. As part of his duties as the communications Electronic Material Officer, he learned about classified material, including procedures to safeguard it.[(7)] He retired from the Navy as a Lieutenant Commander in 1994 after 30 years of service.[(8)] While in the Navy, he held a top secret clearance.[(9)] He is married and has one child.[(10)]

Applicant now works for a contractor to the Navy.[(11)] His work requires access to classified documents provided by the Navy. He works with classified documents on a daily basis and must follow the established procedures for safeguarding these documents. From 1999 through 2004, he worked as a team leader.[(12)] As such, he was responsible for security violations of his team members.[(13)] Individually and as a team leader, he reported security violations he perceived or actually observed.[(14)]

Applicant's duties required him to scan and retrieve relevant messages received by the Navy regarding his work.[(15)] Three times a week, he visited the Navy Command office to review these messages, which numbered between 1,000 and 2,000 each visit.[(16)] Navy staff provided him access to their computers for a short period of time during his visits.[(17)] He scanned the messages, reading the heading or banner, then selected the messages he wanted downloaded.[(18)] He provided this information to a Navy staffer who would download the message, place it in a package, and seal the package which was then double wrapped.[(19)] He did not review the full context of the messages before having them downloaded, packaged and sealed.[(20)] He took the package to his Facility Security Officer to be opened and inventoried.[(21)] On some occasions, he would simply pick up a sealed and wrapped package which he took back to his Facility Security Officer to open and inventory.[(22)]

Security violations

In September 1999, because he was a team leader, Applicant reported to his Facility Security Officer that two classified and confidential messages received on June 9, 1999, were missing.[(23)] His office received these messages in a bundle of classified and unclassified messages, which were then inventoried in a batch with the same control number assigned to all documents.[(24)] His office mate acknowledged working with the messages and placing both with other unclassified messages to be destroyed.[(25)] The employer investigated this incident. In its report to the Defense Security Service, the employer concluded that security had not been compromised, because the messages were written in a code which could only be read by a specific computer program, and most likely had been destroyed with other documents.[(26)] The Defense Security Service agreed.[(27)] As a team leader, Applicant was responsible for this problem, even though he was not directly involved in the misplacement of the documents.[(28)] Following this incident, he recommended that the batch inventory system be replaced with an individual serialization process which would number each message with its own control number.[(29)] This process has been implemented.[(30)]

In November 1999, Applicant visited the Navy Command to review messages and select messages relevant to his work. Once Navy staff prepared the sealed package with his messages, he returned to his work site and gave the sealed package to his Facility Security Officer to open and inventory.[(31)] During this process, his Facility Security Officer found a "NATO confidential" message within the documents.[(32)] Applicant was not aware of the existence of this document until advised by the Facility Security Officer because the marking indicating "NATO confidential" was embedded in the body, not in the heading or banner, of the message.[(33)] At this time, neither he nor his company were authorized to receive any "NATO confidential" messages or documents.[(34)]

Applicant spoke with the Navy staff about the presence of a "NATO confidential" message. The Navy staff advised that 1) "NATO confidential" meant the message originated in a NATO country; 2) its computer system would filter out any "NATO confidential" messages originating in a NATO country; 3) in originating messages, the Navy would label "NATO confidential" in order to send the message out; and 4) the message involved in this incident had been readdressed by the Navy, thus, the label containing "NATO confidential" would be in the body of the message, not in the heading or banner.[(35)] The employer wrote up the incident, and reported it to the Defense Security Services as required.[(36)] The employer investigated, and determinated that classified information had not been compromised.[(37)]

Subsequent to this incident, Applicant requested his employer to upgrade its contract (DD254) to authorize the company, and thus him, to access "NATO confidential" messages as more and more similar messages would appear in the future.[(38)] His employer agreed. The upgrade to this contract is dated December 17, 1999 and reflected his request.[(39)]

All classified documents needed for his work are kept locked in a safe in Applicant's office. On October 10, 2000, Applicant left work in a hurray without checking to make sure his safe had been closed and locked.(40) When he reported to work the next day, he unlocked his office door, then discovered that the safe was not locked.(41) He immediately reported this matter to the Facility Security Officer, who investigated this incident.(42) The investigation determined that classified information had not been compromised.(43) Applicant received an oral reprimand.(44) He also accepts full responsibility for this incident.(45)

On November 3, 2000, the Facility Security Officer recommended Applicant be orally reprimanded for the September 1999 missing classified documents, bringing in the "NATO confidential" message, and leaving the safe open.(46) He also recommended a written reprimand be made a part of his personal folder, briefing on proper security procedures and a one-day suspension.(47) His division manager, a retired Navy Captain, rejected the recommended disciplinary action since most of these incidents were not the result of Applicant's conduct.(48) He authorized only an oral reprimand for the safe being left open, which Applicant's supervisor did.(49)

During his visit to Navy Command on May 29, 2001, and as was his usual practice, Applicant scanned and selected the messages he needed.(50) He printed the 20-25 pages of messages, and stamped them confidential.(51) Due to the volume of information collected during this visit, it was inappropriate for him to read the messages until he returned to his work site.(52) The Navy staff packaged and sealed the classified documents printed and stamped by Applicant.(53) He delivered the secured package to the Facility Security Officer, who opened it.(54) While doing the contents inventory, the Facility Security Officer discovered that one of the messages was a "NATO confidential" message.(55) Despite the implemented upgraded contract provision of December 1999,

he concluded that Applicant had improperly transferred the "NATO confidential" message.(56) The subsequent investigation indicated that classified information had not been compromised.(57)

Applicant transported two classified diskettes from the Navy Command to his work site on March 5, 2002. The Navy staff had classified the diskettes as confidential, when they should have been classified secret.(58) Applicant was unaware of the improper classification until he started printing the documents from a computer cleared to print confidential documents.(59) He immediately reported the security problem.(60) After an investigation, the Facility Security Officer concluded that classified information had not been compromised.(61)

After this incident, the Facility Security Officer again recommended that Applicant be orally reprimanded for all of the security violations involving Applicant, even though other parties actually violated security procedures.(62) He also recommended a written reprimand be made a part of his personal folder, briefing on proper security procedures, and a

one-day suspension.[(63)] His division manager again rejected the recommended disciplinary action.[(64)] He authorized only an oral reprimand for the 2002 incident.[(65)]

Applicant's supervisor and his division manager, a retired Navy Captain, testified on his behalf. Both recommend him for a security clearance because he is honest, forthright, industrious, reports security problems, and accepts responsibility.[(66)] He is not a security risk; rather he is very aware of the various security needs.[(67)] In addition, a senior vice president, whose duties include oversight of security, testified and recommended him for a security clearance.[(68)] She supported his testimony that many of the security violation incidents were not the result of his conduct, but exist because he reported them.[(69)] All three testified that he is a self-reporter of violations, and that there have been no complaints or violations in the last three or four years.[(70)]

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines which must be considered in the evaluation of security suitability. An administrative judge need not view the adjudicative guidelines as inflexible ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines, when applied in conjunction with the factors set forth in the adjudicative process provision in Paragraph E2.2., Enclosure 2 of the Directive, are intended to assist the administrative judge in reaching fair and impartial common sense decisions.

Included in the guidelines are disqualifying conditions and mitigating conditions applicable to each specific guideline. Although the presence or absence of a particular condition or factor for or against clearance is not outcome determinative, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance. In addition, each security clearance decision must be based on the relevant and material facts and circumstances, the whole-person concept, and the factors listed in the Directive. Specifically, these are: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.[(71)]

The sole purpose of a security clearance determination is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.[(72)] The government has the burden of proving controverted facts.[(73)] The burden of proof is something less than a preponderance of the evidence.[(74)] Once the government has met its burden, the burden shifts to the applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.[(75)] Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[(76)]

No one has a right to a security clearance,[(77)] and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[(78)] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[(79)] Section 7 of Executive Order 10865 specifically provides industrial security clearance decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." The decision to deny an individual a security clearance is not necessarily a determination as to the allegiance, loyalty, and patriotism of an applicant.[(80)] It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Based upon a consideration of the evidence as a whole, I find the following adjudicative guideline most pertinent to an evaluation of the facts of this case:

Security Violations - Guideline K: Noncompliance with security regulation raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

CONCLUSIONS

Upon consideration of all the facts in evidence, and after application of all appropriate adjudicative factors, I conclude the following with respect to the allegations set forth in the SOR:

The government has not established its case as to allegation 1.a. Intervening factors, not Applicant's conduct, caused the loss of two classified messages. His office mate has acknowledged that he, not Applicant, placed the two missing classified security messages in a stack of unclassified documents. Part of the reason for this mix up was the security process used in the facility security office. At the time of this 1999 incident, the facility security office inventoried security messages by a batch inventory process which mixed classified and unclassified messages together with the same control number. This inventory system caused confusion with identifying and separating classified documents. Applicant's acceptance of responsibility for his office mate's error is admirable, but does not establish the government's case. Allegation 1.a. is found in favor of the Applicant.

Likewise, the government has not established its case as to allegation 1.d. After he inadvertently printed and transported messages which included a messages marked "NATO confidential" to his work site in 1999, Applicant discussed the

problem with the Navy. He learned that this problem would likely occur in the future. He recommended to his employer that their contract with the Navy be upgraded to allow the company access to "NATO confidential" messages. The contract change is marked December 17, 1999, and was in effect in May 2001, when he is alleged to have improperly received and transported a "NATO confidential" message. When his Facility Security Officer opened the package and began to inventory the messages, this message was found. He did not violate security procedures in 2001 because the upgraded contract allowed him access to these messages. This allegation is found in favor of Applicant.

The government has established its case under Guideline K, as to allegations 1.b. through 1.c., and 1.e. through 1.g.[(81)] Over a three-year period of time, Applicant transported a "NATO confidential" message, left the safe in his office unlocked overnight; and transported a confidential diskette with secret information. His facility Security Officer twice recommended oral reprimands, written reprimands to be placed in his personnel folder, a one-day suspension, and security briefing reviews. These are multiple security violations, which were not deliberate. The unlocked safe incident is the result of negligence. Security Violations Disqualifying Condition (SV DC) E2.A11.1.2.2. (*Violations that are deliberate or multiple or due to negligence*) applies.

Applicant readily admits that he failed to properly lock the safe in his office in October 2000. The office door, however, was locked, and upon his arrival at work the next morning, he discovered the violation and immediately reported it, when he could have simply closed the safe and no one would have known about the violation. A similar incident has not occurred since this date. Security Violations Mitigating Condition (SV MC) E2.A11.1.3.2. (*Were isolated or infrequent*) applies.

The printing and transport of the "NATO confidential" message in 1999 and the diskette in 2002 occurred as the result of mislabeling by the Navy. Because he had to read between 1000 and 2000 messages on each visit to Navy Command, he could not read all messages in full. He, instead, relied upon the necessary information about the message being in the heading or banner. When the Navy readdressed messages, it failed to properly place the document classification in the heading or banner, as it should have done. The Navy marked the diskette confidential, when it should have been marked secret. Applicant had no control over either of these incidents, and was not at fault in either of these security violations. He has mitigated the government's security concerns as to these incidents.

Likewise, Applicant has mitigated the government's security concerns regarding the Facility Security Officer's recommended disciplinary actions. The evidence of record clearly indicates that Applicant is responsible for only one security violation, not the numerous violations alleged by the Facility Security Officer. Rather than address and resolve the problems which caused the security violations, the Facility Security Officer sought to discipline Applicant for the failure of others and without an appropriate basis. Applicant, on the other hands, determined the source of the problems and recommended changes in procedures to prevent further security violations.

After he inadvertently brought the first "NATO confidential" message to his work site, he not only determined how the problem occurred, he recommended that his employer upgrade their contract with the Navy to allow it to have access to "NATO Confidential" messages, as he knew the problem would occur in the future. His employer agreed and obtained the upgrade to its contract. He suggested his employer change its method of inventory of messages from a batch control

number to individual control number for each document, which was done. His managers clearly believe that he is very security conscious, and positive on his security responsibilities. They do not believe he is a security risk. Rather, they view him as an asset to the company, and recommend he get a security clearance. SV MC E2.A11.1.3.4. (*Demonstrate a positive attitude towards the discharge of security responsibilities*) applies. Applicant has mitigated the government's security concerns under Guideline K. Accordingly, for the reasons stated, I find that it is clearly consistent with the national interest to grant a security clearance to Applicant.

FORMAL FINDINGS

Formal findings For or Against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K (Security Violations): FOR APPLICANT

Subparagraph 1.a: For Applicant

Subparagraph 1.b: For Applicant

Subparagraph 1.c: For Applicant

Subparagraph 1.d: For Applicant

Subparagraph 1.e: For Applicant

Subparagraph 1.f: For Applicant

Subparagraph 1.g: For Applicant

DECISION

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant a security clearance for Applicant. Clearance is granted.

Mary E. Henry

Administrative Judg

1. Applicant's 3 page response to SOR, dated September 30, 2005, at 1-3.

2. Government Exhibit 1 (Applicant's security clearance application, dated November 5, 2002) at 1.

3. *Id*. at 1-2.

4. *Id*. at 1.

5. *Id*. at 1, 4; Tr. at 87.

6. Tr. at 87.

7. *Id.*

8. *Id*. at 88; Government Exhibit 1, *supra* note 2, at 4.

9. Tr. at 87.

10. Government Exhibit 1, *supra* note 2, at 2-3.

11. *Id*. at 1.

12. Applicant Exhibit B (Response to SOR with 68 pages of attachments, dated September 30, 2005) at 7.

13. *Id*.

14. Tr. at 91-92.

15. *Id*. at 112, 114-115, 119-120.

16. *Id*. at 125-126.

17. *Id*. at 112, 114-115, 119-120, 125-128.

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id*. at 119-120.

22. *Id*. at 125-128.

23. *Id*. at 34-35, 91-92; Applicant Exhibit A (Notarized statement from office mate, dated March 16, 2006) at 1; Government Exhibit 3 (Employer letter, dated October 19, 1999, regarding investigation into missing messages) at 1.

24. Tr. at 68-72; Applicant Exhibit B, *supra* note 12, at 5.

25. Applicant Exhibit A, *supra* note 23, at 1.

26. Government Exhibit 3, *supra* note 23, at 1.

27. Tr. at 20-21.

28. *Id*. at 91-92.

29. Applicant Exhibit B, *supra* note 12, at 4, 15-16.

30. *Id.*; Tr. at 129.

31. Tr. at 93-94.

32. *Id*.

33. *Id*. at 34-35, 127; Government Exhibit 2 (Applicant's signed statement, dated December 12, 2003) at 3.

34. Tr. at 95-96.

35. *Id*. at 93-94; Applicant Exhibit B, *supra* note 12, at 22.

36. Tr. at 24-25, 34-35.

37. *Id*.

38. *Id*. at 95-96; Applicant Exhibit B, *supra* note 12, at 33-34.

39. Applicant Exhibit C (Copy of DD 254 with employer) at 2.

40. Tr. at 96-98; Government Exhibit 2, *supra* note 33, at 6.

41. Government Exhibit 2, *supra* note 33, at 6; Government Exhibit 4 (Incident report of program manager to Facility Security Officer, dated October 13, 2000) at 1; Government Exhibit 5 (Incident report of Facility Security Officer, dated November 1, 2000) at 1.

42. *Id*.; Tr. at 96-98.

43. Government Exhibit 5, *supra* note 41, at 1.

44. Tr. at 60, 78.

45. *Id*. at 96-98.

46. Government Exhibit 5, *supra* note 41, at 2.

47. *Id*.

48. Tr. at 77-78, 82.

49. *Id*. at 60, 78.

50. Government Exhibit 7 (Incident report of Facility Security Officer, dated June 8, 2001) at 1; Applicant Exhibit B, *supra* note 12, at 29; Government Exhibit 8 (Incident report of Facility Security Officer to Defense Securities Services, dated June 12, 2001).

51. Applicant Exhibit B, *supra* note 12, at 29.

52. *Id*.

53. *Id*.

54. *Id*.

55. Government Exhibit 7, *supra* note 50, at 1; Government Exhibit 8, *supra* note 50, at 1.

56. *Id*.; Applicant Exhibit C, *supra* note 39.

57. Government Exhibit 7, *supra* note 50, at 1; Government Exhibit 8, *supra* note 50, at 1.

58. Tr. at 19-20, 100-101.

59. Government Exhibit 9 (Incident report of Facility Security Officer, dated March 12, 2002) at 1.

60. *Id*.

61. *Id.*

62. *Id*.

63. *Id*.

64. Tr. at 77-78, 82.

65. *Id*. at 78.

66. *Id*. at 54, 77-79, 82

67. *Id.*

68. *Id*. at 24.

69. *Id*. at 22-24.

70. *Id*. at 22-24, 55, 61, 79.

71. Directive, Enclosure 2, ¶ E2.2.1.1. through E2.2.1.9.

72. ISCR Case No. 96-0277 (July 11, 1997) at 2.

73. ISCR Case No. 97-0016 (App. Bd., December 31, 1997) at 3; Directive, Enclosure 3, ¶ E3.1.14.

74. *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

75. ISCR Case No. 94-1075 (App. Bd., August 10, 1995) at 3-4; Directive, Enclosure 3, ¶ E3.1.15.

76. ISCR Case No. 93-1390 (App. Bd. Decision and Reversal Order, January 27, 1995) at 7-8; Directive, Enclosure 3, ¶ E3.1.15.

77. *Egan*, 484 U.S. at 531.

78. *Id*.

79. *Id*.; Directive, Enclosure 2, ¶ E2.2.2.

80. Executive Order No. 10865 § 7.

81. I note that in allegations 1.b., 1.c. and 1.e., the SOR alleges a violation of the National Industrial Security Program Operating Manual (NISPOM), ¶ 5-100. This paragraph discusses very general, non-specific, and superficial security violations. It is unclear how the acts identified in the allegations relate to ¶ 5-100 of NISPOM. In addition, the relationship between the security violation in allegation 1.c. and ¶ 5-304 of NISPOM is unclear.